**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

SRI INTERNATIONAL, INC.,)
a California Corporation,)
)
Plaintiff and)
Counterclaim-Defendant,)
)
v.) C. A. No. 04-1199 (SLR)
)
INTERNET SECURITY SYSTEMS, INC.,) **PUBLIC VERSION**
a Delaware Corporation, INTERNET)
SECURITY SYSTEMS, INC., a Georgia)
Corporation, and SYMANTEC)
CORPORATION, a Delaware Corporation,)
)
Defendants and)
Counterclaim-Plaintiffs.)

OPENING BRIEF IN SUPPORT OF DEFENDANT ISS'S MOTION FOR SUMMARY JUDGMENT THAT THE ASSERTED CLAIMS OF THE SRI PATENTS-IN-SUIT ARE NOT INFRINGED OR, IN THE ALTERNATIVE, ARE INVALID

OF COUNSEL:

Holmes J. Hawkins III
Bradley A. Slutsky
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600

Theresa A. Moehlman
Bhavana Joneja
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com

*Attorneys for Defendants
INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation, and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia corporation*

Dated: June 16, 2006
Public Version Dated: June 23, 2006

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

RULES AND STATUTES

Defendants Internet Security Systems, Inc., a Georgia corporation and Internet Security Systems, Inc., a Delaware corporation, (collectively, "ISS") submit this motion, pursuant to Fed. R. Civ. P. 56, for an Order granting summary judgment that the claims of the four patents-in-suit assigned to Plaintiff SRI International ("SRI") are not infringed or, in the alternative, are invalid.

I. NATURE AND STAGE OF THE PROCEEDINGS

The four patents-in-suit are U.S. Patent Nos. 6,484,203 ("the '203 patent"), 6,711,615 ("the '615 patent"), 6,708,212 ("the '212 patent") and 6,321,338 ("the '338 patent"). (Moore Decl.[1] Exs. A-D [patents-in-suit].) All four patents claim priority from the same application and share an almost identical written description. The first application from which all patents claim priority was filed on November 9, 1998.

Fact and expert discovery has closed. During expert discovery, SRI limited its infringement contentions to the following:

- SRI accuses the configuration of ISS Sensors[2] operating in combination with SiteProtector SecurityFusion Module 2.0 ("Fusion") of infringing:

  '203 claims 1-2, 4-6, 12-13 and 15-17
  '615 claims 1-2, 4-6,13-14, 16-18.

- SRI accuses the Proventia Anomoly Detection System ("ADS") operating in Standalone Mode of infringing '338 claims 1, 4, 5, 11-13, 18, 19 and 24.

- Although SRI made accusations on the '212 patent in the past, its expert offered no infringement opinions with respect to this patent. ISS seeks a declaratory judgment that the claims of the '212 patent are not infringed and are invalid.

[1] Filed contemporaneously herewith.

[2] The ISS Sensors include RealSecure sensors (Network Sensor, Guard, Server Sensor, and Desktop) and Proventia sensors (A, G, M, Server, and Desktop).

II. SUMMARY OF THE ARGUMENT

The patents-in-suit generally relate to detecting intrusions in networked computing environments, a field known as network intrusion detection. There are two main facets to the patents-in-suit: (1) an architecture for hierarchical event monitoring and analysis in an enterprise network and (2) a statistical algorithm for use in detecting attacks. The '203 and '615 patent claims focus on the architecture; the '338 patent claims focus on the statistical algorithm and the '212 patent claims include both facets.

A. Hierarchical Architecture Claims

ISS was a pioneer in the network intrusion detection field. Its early products were sold more than one year before SRI filed its original patent application. Therefore, those products are prior art to the SRI patents-in-suit under 35 U.S.C. §102(b).

[redacted]. In the original version of the ISS product, the sensors were called RealSecure and the centralized management system was called Console. Today, the ISS sensors run on various platforms and the centralized management system is called SiteProtector. The ISS Sensors and centralized management system are, and have always been, specialized components that are optimized for the tasks that they perform.

The hierarchical architecture claims of the patents-in-suit call for a different architecture. The patents' architecture is made up of generic ***monitors*** that can be configured to operate anywhere in an analysis hierarchy. As set forth in Defendants'

Opening Claim Construction Brief, Defendants construe ***monitor*** according to the definition provided in the specification:

> ***Monitor/Network Monitor:*** Generic code that can be dynamically configured and reconfigured with reusable modules that define the monitor's inputs, analysis engines and their configurations, response policies and output distribution for its reports.

Under this construction of ***monitor***, as SRI's expert admitted, ISS products do not infringe any of the hierarchical architecture claims (all claims at issue for the '203, '615 and '212 patents). There is no notion of a generic monitor in ISS products.

In an attempt to build an infringement argument, SRI offers a construction of ***monitor*** that essentially would encompass any component that analyzes data. However, in advancing this ***monitor*** construction to read the claims on the current ISS products, SRI also reads those claims on the prior art ISS products. Both have the same architecture of sensors feeding a centralized management system. If the current ISS Sensors and the centralized management system are monitors, then so too are the prior art ISS Sensors and the centralized management system, as reflected in the following chart using claim 1 of the '203 patent:[3]

[3] As described in Defendants' Joint Motion For Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§ 102 & 103, the hierarchical architecture claims of the '203, '615 and '212 patents are extremely redundant. The one difference, however, between the asserted claims of the '203 patent and those of the '615 patent is that the '615 claims specify two more categories of network traffic data that may be analyzed. To meet the claims, only one of those categories need be analyzed. Thus, prior art that analyzes a category listed in the '203 patent would also read on the '615 claims.

'203 Claim 1	Prior Art ISS RealSecure	Current ISS Products
1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	ISS RealSecure Sensors could report detections of suspicious network activity to a centralized management system, Console.	ISS Sensors can report detections of suspicious network activity to a centralized management system, SiteProtector.
deploying a plurality of network monitors in the enterprise network;	A plurality of RealSecure Sensors could be deployed in an enterprise network.	A plurality of ISS Sensors could be deployed in the enterprise network.
detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories ... [list of categories];	RealSecure Sensors used signature and protocol based analysis to detect known patterns of attack using one or more of the listed categories of network traffic data.	ISS Sensors use signature and protocol based analysis to detect known patterns of attack using one or more of the listed categories of network traffic data.
generating, by the monitors, reports of said suspicious activity; and	RealSecure Sensors generate alerts when a pattern is detected and send the alerts to Console.	ISS Sensors generate alerts when a pattern is detected and send the alerts to SiteProtector.
automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	Console automatically receives the reports and combines them on its display based on various criteria (called "roll-up").	SiteProtector automatically receives the reports and combines them based on various criteria (called "roll-up").

Recognizing this dilemma, SRI has restricted its infringement contentions to a particular configuration of ISS products: ISS Sensors in combination with the SiteProtector SecurityFusion Module 2.0 ("Fusion"). Fusion is an add-on product to SiteProtector. SRI does not accuse ISS Sensors working with SiteProtector alone of infringement. Fusion 2.0 includes two components -- Impact Analysis and Attack Pattern. SRI's expert confirmed that SRI only accuses the combination when Attack Pattern is operating.[4] These limitations do not get SRI anywhere. SRI faces the same dilemma -- either its claims are not infringed (if SRI's construction of ***integrating*** is

[4] *See* Moore Decl. Ex. E [Kesidis Dep.] at pp. 151-52.

adopted) or they are invalid based on the prior art RealSecure products (if Defendants' construction of ***integrating*** is adopted).

SRI's construction of ***integrating*** requires that the reports be combined into "another functional unit". According to SRI's expert, a functional unit is a "meta-alert" that can undergo further processing.[5] [redacted]. The early ISS Console also provided similar roll-up functionality when it combined related events.

Defendants' construction of the term ***integrating*** is more in accord with its plain meaning and does not require that another "functional unit" be generated. Under Defendants' construction, the claims would be anticipated by the prior art RealSecure products, which performed ***integration***. The Console combined the reports of detected suspicious network activity and determined relationships among the reports based on various criteria. SRI's expert admitted that this functionality would meet the ***integrating*** step under the Defendants' construction.[6]

[5] Moore Decl. Ex. E [Kesidis Dep.] at p. 309:7-16 ("an instance of a functional unit is a report of suspicious activity that -- as you would receive from a network service monitor. So that in turn, for example, you could dispatch an integrated report or a meta-alert, say, to a peer hierarchical monitor or a hierarchical monitor at a -- at a higher layer. So I would describe 'functional unit' as, by example, a meta-alert or a meta report of suspicious activity.").

[6] Moore Decl. Ex. E [Kesidis Dep.] at pp. 327:9-328:25.

Thus, no matter which claim constructions are adopted, summary judgment is appropriate here:

- Defendants' construction of *monitor* adopted -- no infringement of any of the '203, '615 and '212 claims;

- SRI's construction of *monitor* and *integrate* adopted -- no infringement of the '203, '615 and '212 claims;

- SRI's construction of *monitor* and Defendants' construction of *integrate* adopted -- invalidity of the '203 and '615 claims[7] based on the prior art RealSecure system.

Moreover, during discovery, SRI did not prove direct infringement. Because the hierarchical architecture claims at issue are method and system claims, and ISS sells components, SRI alleges contributory infringement and inducement. SRI must still show direct infringement. [redacted]. Without direct infringement, SRI cannot make its case. Summary judgment of non-infringement is appropriate on this ground as well.

B. Statistical Algorithm Claims

This spring ISS introduced the Proventia ADS product. SRI accuses this product of infringing '338 patent claims 1, 4, 5, 11-13, 18, 19 and 24.[8] ADS does not meet these claim limitations.

[7] The '212 patent claims all require that a statistical detection method be employed. [redacted].

[8] SRI does not accuse ADS of infringing the '212 claims, which include both the hierarchical architecture facet and the statistical detection method. [redacted]

All asserted '338 claims require the limitation of *determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.* [redacted]. It, therefore, does not meet the claims.

Moreover, if Defendants' construction of the *determining* claim limitation is adapted, ADS would not infringe for an additional reason. As set forth in the patent specification, this *determining* step requires no prior knowledge of what constitutes suspicious activity. The algorithm figures out what that is by automatically computing a historically adaptive threshold from the empirical data. [redacted] ADS, therefore, does not meet this claim element literally or under the doctrine of equivalents.

Moreover, every asserted '338 claim includes the element of *receiving network packets handled by a network entity.* [redacted] Thus, it does not receive *network packets* in this mode. [redacted]. Thus, [redacted] and, therefore, does not receive network packets *handled by a network entity*

[redacted].

Thus, there is no infringement of the asserted '338 patent claims by ADS.

III. STATEMENT OF FACTS

A. The Prior Art ISS Products

Prior to November 9, 1997, various versions of the ISS RealSecure system were commercially on sale, including RealSecure NT 1.0 and RealSecure UNIX 1.2.1, 1.1.1, and 1.0. (Hall Decl.[9] ¶ 21 and ¶¶ 6, 7, 12, 14, 19, 20, Exs. A-B, G, J, N, O.) Prior to November 9, 1997, ISS also provided manuals of how these systems operated not only to its customers, but also off of its website. (Hall Decl. ¶¶ 8-17, Exs. C, F, M and ¶ 22, 23.)

The prior art RealSecure sensors (also called engines) analyzed network packets in real time and provided security and intrusion reports to the Console, a centralized administrators' or management module. (Hall Decl. ¶ 4.) The Console could have many RealSecure sensors under its control. (*Id.*) The Console integrated the reports from the RealSecure sensors and provided correlation capabilities. (Hall Decl. ¶ 5.)

For example, the Console could correlate reports based on various criteria, including the network source address that initiated the security incident ("Source"), the network destination address affected by the security incident ("Destination"), and the name of the security attack event recorded ("Event"). This correlation was shown in an Activity Tree Window display, which was automatically produced upon startup of the RealSecure Console and automatically updated without manual intervention. (*Id.*) On this Activity Tree Window, the Console could display the grouping and numerical count of all similar intrusion events. (*Id.*)

[9] Filed contemporaneously herewith.

B. [redacted]

[redacted]

[redacted] ISS Sensors report to a management console, SiteProtector.

[redacted]

[10] Filed contemporaneously herewith.

[redacted]

The PAM component is designed and built to detect instances of known attack patterns. Instances of known attack patterns are not "suspicious," they require no further investigation to determine whether something bad has occurred. Each attack pattern describes something known and defined by policy to be itself a misuse, so each detected instance of an attack pattern is itself a misuse.

[redacted]

[redacted]

[redacted]

[11] Filed contemporaneously herewith.

[redacted] SRI does not accuse Fusion of infringement when only Impact Analysis is running.

[redacted]

[redacted]

[redacted]

C. Proventia ADS

[redacted]

The Collectors provide NetFlow data to the Analyzer. [redacted]

> "NetFlow is a traffic profile monitoring technology developed by Darren Kerr and Barry Bruins at Cisco Systems, back in 1996. As a de facto industry standard, NetFlow describes the method for a router to export statistics about the routed socket pairs, and it's now a built-in feature for most Cisco routers as well as Juniper, Extreme and some other vendor's routers and switches."

(Moore Decl. Ex. H [SecurityFocus 1796].) These summary records are "exported" (transmitted) from the router to any IP address configured in the router/switch to receive them.

[redacted]

[12] Filed contemporaneously herewith.

[redacted]

[redacted]

D. The Patents-In-Suit

As discussed in detail in the Defendants' Opening Claim Construction Brief, the specification of the patents-in-suit disclose a network monitoring system for an enterprise domain that employs an analysis hierarchy of monitors. All claims of the '203, '615 and '212 patents include this monitor architecture.

The patent specification defines monitor to consist of generic code that can be dynamically configured and reconfigured with a reusable module that the patent calls a "resource object". (Moore Decl. Ex. A ['203 patent] at col. 10:29-33 and 10:52-58.) The monitor's generic code includes analysis engines and a resolver that implements a response policy. (*Id.* at col. 4:5-15.) The configuration data for the generic monitor in the resource object includes: what data the monitor will take as input; the configurations of monitors' analysis engines; any response policies the monitor will implement; and the other monitors to which it will provide its analysis reports. (*Id.* at col. 10:52-col. 11:61.) Through this process, the monitors are configured to analyze and respond to network activity and to interoperate to form the analysis hierarchy. (*Id.* at col. 2:56-59.)

According to the specification, this reusable software architecture has many advantages. It enables an analysis hierarchy to be formed, providing "a framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an enterprise network." (*Id.* at col. 2:58-63.) It allows reuse of modules, which the patent specification states "reduce[s] implementation and maintenance efforts." (*Id.* at col. 10:33-37 and 10:48-51.) Finally, the monitor can be easily reconfigured by modifying its resource object, which allows for adaptive analysis. (*Id.* at col. 11:62-67.)

As discussed in the Defendants' Opening Claim Construction Brief, the patent discloses two types of analysis units for the monitor -- statistical detection (also known as "anomaly detection") and signature detection (also known as "rule-based" or "threshold" detection). (*See* Moore Decl. Ex. D ['338 patent] at Figure 2.)

The claims of the '338 patent relate to the algorithm used by the statistical anomaly detection unit. The claims of the '212 patent also includes a requirement that at least one network monitor utilize a statistical detection method.

The statistical algorithm defined in the patent includes several steps. It automatically generates and updates a long-term statistical profile of network activity based on certain network measures to represent "normal activity." (*Id.* at col. 2:42-46.) It also automatically generates a short-term statistical profile of network activity to represent "recent activity." (*Id.* at col. 6:44-47.) The short-term and long-term statistical profiles are then compared. If the difference is "significant", the algorithm determines that there is suspicious network activity. (*Id.* at col. 6:44-47; *see also* Figs. 4 and 5.) The difference will be considered "significant" when it exceeds an historically adaptive threshold that is empirically determined to be statistically significant. (*Id.* at col. 6:59-67.) This threshold is "adaptive" because it changes over time based on the history of events -- when behavior changes over time, the algorithm will adjust the threshold according to the empirical data.

The patent states that the advantage of this method is that it requires no prior knowledge of intrusive or exceptional activity. (*Id.* at col. 6:57-58.) According to the specification, the advantage of this method is that it requires no prior knowledge of intrusive or exceptional activity. (*Id.* at col. 6:57-58.) Instead, what constitutes suspicious network activity is "learned" based on observed data over time.

In contrast, the patent identifies basic threshold analysis as a signature based technique. (*Id.* at 7:46-47.) As the patent states, signature analysis "maps an event stream against abstract representations that are known to indicate undesirable activity." (*Id.* at 7:46-47.)

IV. THE APPLICABLE LAW

A. The Standard For Summary Judgment

Rule 56(c) mandates that summary judgment "is appropriate" if the pleadings and affidavits, if any, "show that there is no genuine issues as to any material fact." Rule 56(c), Fed. R. Civ. P. The standard for summary judgment in a patent case is the same as in any other type of action. *Union Carbide Corp.* v. *Am. Can Co.*, 724 F.2d 1567, 1571 (Fed. Cir. 1984). The Federal Circuit has repeatedly stated that "[s]ummary judgment is as appropriate in a patent case as in any other." *Desper Prods.* v. *Qsound Lab.*, 157 F.3d 1325, 1332 (Fed. Cir. 1998).

To defeat ISS's summary judgment motion, SRI must present sufficient evidence to support a reasonably jury finding in its favor. *See Anderson* v. *Liberty Lobby, Inc.*, 477 U.S. 242, 249-50 (1986). Notwithstanding that legitimate evidentiary inferences must be drawn in the non-movant's favor, the plaintiffs cannot create a genuine issue of material fact merely by stating that a fact is challenged. *Barmag Barmer Maschinenfabrik AG* v. *Murata Mach., Ltd.*, 731 F.2d 831, 835-36 (Fed. Cir. 1984); *see also Moore U.S.A., Inc.* v. *Standard Register Co.*, 229 F.3d 1091, 1112 (Fed. Cir. 2000) ("A party may not overcome a grant of summary judgment by merely offering conclusory statements."). Moreover, "[e]ven disputed material facts will not defeat summary judgment when, taking all factual inferences in favor of the nonmovant, the moving party is nonetheless entitled to judgment as a matter of law." *Spectrum Int'l, Inc.* v. *Sterilite Corp.*, 164 F.3d 1372, 1378 (Fed. Cir. 1998).

B. The Law On Infringement

A patent infringement analysis is a two-step process: (1) claim construction and (2) application of the properly construed claims to the accused product. *Markman* v. *Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995) (*en banc*), *aff'd*, 517 U.S. 370 (1996). "While claim construction is a question of law, infringement, whether literal or under the doctrine of equivalents, is a question of fact." *Moore*, 229 F.3d at 1105 (internal citations omitted).

"To establish infringement, all of the elements of the claim, as correctly construed, must be present in the accused system." *TechSearch L.L.C.* v. *Intel Corp.*, 286 F.3d 1360, 1371 (Fed. Cir. 2002). "If even one limitation is missing or not met as claimed, there is no literal infringement." *Mas-Hamilton Group* v. *LaGard, Inc.*, 156 F.3d 1206, 1211 (Fed. Cir. 1998) (citing *Pennwalt Corp.* v. *Durand-Wayland, Inc.*, 833 F.2d 931, 934 (Fed. Cir. 1987) (*en banc)*). Where, as here, there is no legitimate dispute as to the nature of the accused product, "the question of literal infringement collapses to one of claim construction and is thus amenable to summary judgment." *Athletic Alternatives, Inc.* v. *Prince Mfg., Inc.*, 73 F.3d 1573, 1578 (Fed. Cir. 1996). Accordingly, where a Court determines that a structure of the accused device does not meet a properly construed claim limitation, summary judgment of noninfringement is appropriate. *Gentex Corp.* v. *Donnelly Corp.*, 69 F.3d 527, 530 (Fed. Cir. 1995).

An accused product that does not literally infringe the claims of a patent may still infringe under the doctrine of equivalents if each limitation in the claim is present in the accused product either literally or equivalently. *See, e.g.*, *Marquip, Inc.* v. *Fosber Am., Inc.*, 198 F.3d 1363, 1366 (Fed. Cir. 1999); *see also Kustom Signals, Inc.* v. *Applied*

Concepts, Inc., 264 F.3d 1326, 1333 (Fed. Cir. 2001) ("The all-elements rule is that an accused device must contain every claimed element of the invention or the equivalent of every claim element.") (internal citations omitted). An element in the accused product is equivalent to a claim limitation only if the differences between them are "insubstantial" to one of skill in the art. *See., e.g., Marquip, Inc.*, 198 F.3d at 1366. The doctrine of equivalents, however, "cannot allow a patent claim to encompass subject matter that could not have been patented . . . . Thus, we have held that the doctrine of equivalents cannot allow a patent to encompass subject matter existing in the prior art." *K-2 Corp.* v. *Salomon S.A.*, 191 F.3d 1356, 1367 (Fed. Cir. 1999).

C. The Law On Invalidity

Patent invalidity may also be addressed by summary judgment. *U.S. Gypsum Co.* v. *National Gypsum Co.*, 74 F.3d 1209, 1212 (Fed. Cir. 1996). Although the claims of an issued patent are presumed to be valid, this presumption is rebuttable by clear and convincing evidence. *Id.*

Under 35 U.S.C. §102(b), a person is not entitled to a patent on an invention that was "described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application."

A patent is anticipated when a "prior art" device or reference reveals each and every element or limitation of the claimed invention. *Schering Corp.* v. *Geneva Pharms.*, *Inc.*, 339 F.3d 1373, 1377 (Fed. Cir. 2003); *Constant* v. *Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1570 (Fed. Cir. 1988); *Azko N.V.* v. *United States Int'l Trade Comm'n*, 808 F.2d 1471, 1479 (Fed. Cir. 1986). Stated another way, "anticipation" and "infringement" are reciprocals, *i.e.*, a structure or a method in a prior art device or reference that would "infringe" a patent claim if later in time, "anticipates" that claimed invention if earlier in time. *Dow Chem. Co.* v. *Astro-Valcour, Inc.*, 267 F.3d 1334, 1339-40 (Fed. Cir. 2001) citing *Lewmar Marine, Inc.* v. *Barient, Inc.*, 827 F.2d 744, 747 (Fed. Cir. 1987). The claims of a patent must be construed the same for purposes of analyzing validity as for infringement. *See Kimberly-Clark Corp.* v. *Johnson & Johnson Co.*, 745 F.2d 1437, 1449 (Fed. Cir. 1984) ("they [the claims] must be construed in the identical way for both infringement and validity").

V. ARGUMENT

A. Either The Current ISS Products Do Not Infringe The Hierarchical Architecture Claims Or The Prior Art ISS Products Anticipate Those Claims

1. Under ISS's Construction Of *Monitor*, There Is No Infringement

All claims of the '203, '615 and '212 patents relate to the hierarchical architecture of monitors. They are extremely redundant. All require ***network monitors*** and ***hierarchical monitors***. A representative claim is claim 1 of the '203 patent:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
>
> deploying a plurality of ***network monitors*** in the enterprise network;
>
> detecting, by the ***network monitors***, suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};
>
> generating, by the monitors, reports of said suspicious activity; and
>
> automatically receiving and ***integrating*** the reports of suspicious activity, by one or more ***hierarchical monitors***.

Defendants, using the definition of ***monitor*** provided in the patent specification, have proposed that ***monitor*** be construed as:

> Generic code that can be dynamically configured and reconfigured with reusable modules that define the monitor's inputs, analysis engines and their configurations, response policies and output distribution for its reports.

Under this definition of monitors, ISS does not infringe. There is no notion of this generic monitor architecture in the ISS products. The ISS products use specialized components optimized for their function. [redacted] SRI's expert conceded at his deposition that the ISS products lack the generic code required for a monitor. (Moore Decl. Ex. E [Kesidis Dep.] at p. 181 ("I found no evidence that SiteProtector or with Security Fusion 2.0 with the attack pattern module, that it used the generic code from the agents [ISS sensors].").) Therefore, ISS products do not infringe the hierarchical claims.

2. Under SRI's Construction Of *Monitor*, The Claims Are Either Not Infringed (SRI's Construction of *Integrate)* Or Are Invalid (Defendants' Construction of *Integrate*)

SRI's construction of ***monitor*** is broader and would encompass both the current ISS products and the prior art ISS RealSecure products:

> Process or component in a network that can analyze data; depending on the context in specific claims, the network monitor may analyze network traffic data, reports of suspicious network activity or both.

In a futile attempt to avoid ensnaring the prior art ISS products, SRI has tried to narrow the construction of the limitation of ***integrating the reports of suspicious activity, by one or more hierarchical monitors.*** SRI construes ***integrating*** as "combining those reports into *another functional unit*."

SRI likely will argue that this construction distinguishes the prior art ISS products, but, if it does, it also distinguishes the current ISS products.

When the Fusion Attack Pattern component detects a pattern [redacted] Thus, there is no infringement under SRI's construction.

SRI implicitly concedes non-infringement because it concedes that SiteProtector acting independently does not infringe. SiteProtector has the "roll-up" ability [redacted] The prior art Real Secure Console had similar roll-up functionality.

If Defendants' construction of ***integrate*** is adopted, then the claims are invalid in light of the prior art ISS RealSecure system. Defendants' construction is the same as SRI's except that it does not require that "another functional unit" be generated. The prior art RealSecure system would meet the limitation, as conceded by SRI's expert. (Moore Decl. Ex. E [Kesidis Dep.] at pp. 327:9-328:25.)

With SRI's construction of ***monitor*** and Defendants' construction of ***integrate***, all asserted claims of the '203 and '615 patents are invalid. This is demonstrated in the invalidity chart adopted by ISS's expert Stephen Smaha, which is attached to the Moore Decl. as Ex. J. As discussed above, the prior art RealSecure system had Sensors reporting to a Console. Under SRI's construction, the Sensors would be the network monitors and the Console would be the hierarchical monitor. [redacted]

[redacted] Thus, the elements of all asserted independent claims of the '203 and '615 patents are present in the prior art RealSecure system. The prior art RealSecure products also met the additional limitations of the asserted dependent claims, as set forth in the invalidity chart.

B. SRI Has Failed To Show Direct Infringement Of The Hierarchical Claims

SRI's hierarchical architecture claims are method and system claims. Thus, SRI has accused ISS of contributory infringement and inducement of infringement because ISS sells component parts. In order to prove its case, SRI must still show direct infringement by an implemented configuration of ISS products. *Anton/Bauer, Inc.* v. *PAG*, Ltd., 329 F.3d 1343 (Fed. Cir. 2003) citing *Carborundum Co.* v. *Molten Metal Equip. Innovations, Inc.*, 72 F.3d 872, 876 n.4 (Fed. Cir. 1995) ("Absent direct infringement of the claims of a patent, there can be neither contributory infringement nor inducement of infringement.").

Here, SRI alleges that the infringing combination is ISS Sensors operating with SiteProtector and with Fusion 2.0 running Attack Pattern Correlation. [redacted]

[redacted]

Discovery has closed. Because SRI will be unable to establish direct infringement, it necessarily will be unable to establish contributory infringement or inducement of infringement. Therefore, ISS is entitled to summary judgment of non-infringement.

C. The Proventia ADS Does Not Infringe The Statistical Algorithm Claims

The ISS Proventia ADS system does not meet the asserted claims of the '338 patent. Claim 1 of the '338 patent requires (emphasized terms not infringed):

> 1. A method of network surveillance, comprising:
>
> > ***receiving network packets handled by a network entity;***
> >
> > building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
> >
> > comparing at least one long-term and at least one short-term statistical profile; and
> >
> > ***determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.***

The only other asserted independent claim is claim 24. This claim is the system version of claim 1 (emphasized terms not infringed):

> 24. A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to:
>
> > ***receive network packets handled by a network entity***;
> >
> > build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the measure monitoring data transfers, errors, or network connections;
> >
> > compare at least one short-term and at least one long-term statistical profile; and

> ***determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.***

The Proventia ADS does not meet the ***receiving/receive*** step of every asserted claim. [redacted]. Thus, there is no infringement.

The Proventia ADS also does not meet the ***determining/determine*** step of the claims. [redacted] Therefore, it does not infringe.

The Proventia ADS also does not meet the ***determining/determine*** step under Defendants' proposed construction, which is the construction that results if the claims are read in light of the specification:

> determining whether the difference between the short-term statistical profile and the long-term statistical profile ***exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation*** between the two profiles, requiring no prior knowledge of suspicious network activity

[redacted]

[redacted] Therefore, Proventia ADS does not infringe for this additional reason if Defendants' proposed construction is adopted.

VI. CONCLUSION

For the foregoing reasons, ISS respectfully requests that the Court grant this motion:

1. With respect to the hierarchical architecture claims of the '203, '615 and '212 patents, ISS requests that:

   a. The Court grant summary judgment of no contributory infringement and no infringement by inducement based on SRI's failure to prove direct infringement;

   b. Depending on the claim constructions adopted by the Court, the Court grant summary judgment that either:

      i. There is no infringement of any of the '203, '615 and '212 patent claims, if Defendants' construction of *monitor* is adopted, or if SRI's constructions of *monitor* and *integrate* are adopted;

      or, alternatively:

      ii. The claims of the '203 and '615 patent are invalid based on the prior art RealSecure system, if SRI's construction of *monitor* and Defendants' construction of *integrate* is adopted.

2. With respect to the asserted claims of the '338 patent, ISS requests that the Court grant summary judgment of non-infringement.

3. With respect to the '212 patent, ISS requests that Court grant summary judgment of non-infringement on the additional ground that the ISS products do not include the statistical detection method of the claims.

OF COUNSEL:

Holmes J. Hawkins III
Bradley A. Slutsky
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600

Theresa A. Moehlman
Bhavana Joneja
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100

Dated: June 16, 2006
Public Version Dated: June 23, 2006

POTTER ANDERSON & CORROON LLP

By: *\/s/ David E. Moore*
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com

Attorneys for Defendants
INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia corporation

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, David E. Moore, hereby certify that on June 23, 2006, the foregoing document was hand delivered to the following persons and was electronically filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following and the document is available for viewing and downloading from CM/ECF:

John Horvath
Fish & Richardson P.C.
919 N. Market Street, Suite 1100
P. O. Box 1114
Wilmington, DE 19899

Richard K. Herrmann
Morris James Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

I hereby certify that on June 23, 2006, I have Electronically Mailed the attached document to the following non-registered participants:

Howard G. Pollack
Michael J. Curley
Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063
pollack@fr.com
curley@fr.com

Paul S. Grewal
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014
pgrewal@daycasebeer.com

/s/ David E. Moore
Richard L. Horwitz
David E. Moore
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 North Market Street
Wilmington, DE 19899-0951
(302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com